Internet computer virus protection policy

H. Joseph Wen
School of Management, New Jersey Institute of Technology, Newark, USA

Organizations and individuals today need to have a comprehensive virus protection policy to face the growing threats of Internet computer viruses. The purpose of this paper is to introduce to the reader the threats that Internet computer viruses can cause and provide guidelines on how organizations or individuals can protect themselves against these viruses. Discusses the full set of virus types. Recommends the development of virus protection policy for organizations.

Introduction

Computer viruses have evolved since first being created and the creators of these virus programs have also become cleverer. Their newer creations are more complex and difficult to detect and remove. They have also broadened their arena of inflicting disaster to encompass the Internet (Nachenberg, 1997; Whalley, 1996).

As companies increasingly embrace Internet technology as a way to conduct global electronic commerce, the possibility of acquiring a computer virus is greater. Computer viruses have become an ongoing worldwide problem and can travel quickly through the Internet, causing even more destruction. On November 2, 1988, the Internet virus, coded in C programming language, invaded ARPANET. Within minutes the Internet network was devastated and many computer centers had to shut down. These included NASA's Ames Laboratory, Lawrence Livermore Laboratory, MIT and the Rand Corporation.

Organizations and individuals today need to have a comprehensive virus protection policy to face the growing threat of these old and new viruses on Internet. The purpose of this paper is to introduce to the reader the threats that Internet computer viruses can cause and provide guidelines on how organizations or individuals can protect themselves against these viruses.

What is a computer virus?

A computer virus is one kind of threat to the security and integrity of computer systems. Like other threats, a computer virus can cause the loss or alteration of programs or data, and can compromise their confidentiality. Unlike many other threats, a computer virus can spread from program to program, document to document and from computer system to computer system, without direct human intervention.

The essential component of a virus is a set of instructions that, when executed, spreads itself to other, previously unaffected, programs or files. A typical computer virus performs two functions. First, it copies itself into previously uninfected programs or files. Second, (perhaps after a specific number of executions, or on a specific date) it executes whatever other instructions the virus author included in it. Depending on the motives of the virus author, these instructions can do anything at all, including displaying a message, erasing files or altering stored data. In some cases, a virus may contain no harmful or disruptive instructions at all. Instead, it may cause damage by replicating itself and taking up system resources, such as disk space, CPU time, or network connections.

There are two ways for a virus to spread: booting from an infected diskette or executing an infected program. Most viruses stay active in memory until you turn off your computer. When you turn off the computer you remove the virus from memory, but not from the file or disk it has infected. The next time you use your computer, the virus program is activated again and attaches itself to more programs. A computer virus is like a biological virus: it lives to replicate.

All computer viruses in existence live in some location on the computer. We are aware of all the areas where computer viruses live and breed. They are located in the hard boot sector of a disk that may include the hard drive, floppy disk or CD. They can also be found in program files. There are five major types of viruses (Jarvis, 1997; Nachenberg, 1997).

1 Boot sector viruses.
2 Program viruses.
3 Stealth viruses.
4 Polymorphic viruses.
5 Multipartite viruses.

A boot sector virus modifies the boot sector and it appears to be the most common virus. Every disk has a boot sector that controls how a computer operates when starting. A boot sector virus loads into memory from the diskette on starting and may infect other applications, other disks or just create poor performance. The infection begins when the computer is turned on and there is a floppy diskette in your drive.

The second category of viruses is program infectors. These viruses live in program files.

Information Management & Computer Security
6/2 [1998] 66–71

[ISSN 0968-5227]

Information Management & Computer Security
6/2 [1998] 66–71

This type of virus loads into memory when the system executes the file. Once in memory, the virus can infect any and all programs subsequently executed. Then those files can infect other program files.

As the name implies, stealth viruses have the characteristic of hiding. A virus with stealth attributes tends to be found in a boot sector or a program file. The majority of known stealth viruses are of the boot sector type because this type is much easier to blend into programs. Stealth viruses cover their trails by two techniques. The first is to redirect disk reads to other locations and the second technique is making a change in boot tables. The virus usually changes file sizes to escape detection.

Polymorphic viruses are viruses that appear different in each infected file, making detection more difficult. They change their characteristics during their replication process. These viruses are the most difficult for anti-virus software packages to detect.

There are several early signs that a computer may be infected with any one of these virus types. Computer viruses are known to display unfamiliar graphics or messages on your computer screen. Viruses are known to reformat hard disks without prompting the user, they change the disk volume label and create unknown files or sub-directories. Performance of computers including speed and memory size is affected and programs or files may get deleted.

The new threat: macro viruses

The most successful computer virus that has caused havoc in corporations and has been responsible for "down time" is the macro virus and its mutation forms.

If a user sends or receives documents or spreadsheets, chances are his/her computer has been or will be infected at one time or another by a macro virus. Relatively new on the computing scene, these computer viruses are spreading faster than most anti-virus software makers can find ways to detect and remove them. Macro viruses are now the most prevalent computer viruses in the world. This is largely due to the new way in which they spread. They attach themselves to word processor and spreadsheet documents, which often are transmitted as e-mail attachments via the Internet and throughout the world. Macro viruses represent 80 percent of all infections (Coursey, 1997). Moreover, the instances of macro virus infections doubled about every four months in 1996. This makes these viruses the fastest to spread.

The most destructive macro virus, by far, is the concept virus. Within months of its discovery in the fall of 1995, the concept virus accounted for more than three times the number of virus encounters reported for the previous leader, the "Form virus." Today, the concept virus has infected almost one-half of all medium to large corporations according to a survey conducted by NCSA.

While most of the known macro viruses (which number over 500) are not destructive, many causes a considerable loss of productivity and staff time. The concept virus restricts file saving operations, and other macro viruses have been known to manipulate information, control data storage, and even reformat hard drives. This potential destructiveness has corporate system administrators trying to find the best way to combat these new virus threats.

Unfortunately, with the ease in which these viruses can be developed, coupled with the vast number of word processing and spreadsheet documents exchanged throughout the world every day via the Internet, it is difficult to detect using anti-virus software. Essentially, macro viruses are spreading and mutating so fast that anti-virus software designed to detect and remove them is obsolete soon after it is shipped to users.

Internet computer viruses

The new wave of computer virus threats will not travel via floppy disks or network files but via the Internet. The threat of Internet viruses is more deadly than any previous computer virus threat seen. These viruses will not only display messages or delete files but their capabilities are far deadlier.

One example of what viruses over the Internet are capable of doing is being able to seek out an Internet user's personal bank account information, without a personal identification or transaction number. This may sound like science fiction, but to the computer virus developer in Germany who created the virus it is not (Chen, 1997; *New York Times*, 1993).

The threat of this Internet virus is that it loads automatically as the user browses the World Wide Web. The virus is carried by a control development using Microsoft's Active X, which is in growing use on Web pages throughout the world. This is only the beginning of the power that Active X can display over the Web. For example an Active X control called "Exploder" can shut down Microsoft Windows 95 and shut down your computer if it has an energy conservation BIOS. This illustrates the power that these "new" viruses can have over the Internet.

Information Management & Computer Security
6/2 [1998] 66–71

Any type of computer is at risk. Even if you have a firewall between the Internet and your computer, you can be at risk.

This threat is not only limited to Active X controls. Similar capabilities are now being attributed to Java, a competing programming language developed by Sun Microsystems.

Active X and Java were not created to transmit viruses but were created for Web page designers to incorporate a wide array of impressive effects on Web pages. They add movement and dimension to previously 'flat' Web pages. Java and Active X are responsible, for example, for the ability for stock prices to scroll across Web pages and for animation of web pages.

The dangers and advantages that viruses have are that to operate properly Active X controls and Java applets need to gain access to your hard disk. Insufficient memory and Internet traffic necessitate this approach. The virus code developers are using this feature of Active X and Java to read, delete or corrupt files, access RAM and access files on computers attached via a LAN.

In the example of the Internet virus from Germany stated previously, the Active X control searches the user's hard disk for installation of Quicken, a popular personal software that is used by over nine million people worldwide. Once the virus locates the Quicken files, the Active X control orders a transfer of funds that is added to the software's list of queued transfers. This is completed unknown to the user when he pays the bills.

Computer viruses were thought to be malicious code that spreads by duplicating itself via attachments to executable files. The first threat of viruses over the Internet came from FTP downloads and reading attachments from e-mail. With the new threat, viruses in Active X controls and Java applets can spread with even no action by the user. Simply surfing the World Wide Web can be dangerous.

Of the two carriers of viruses, Active X is perceived to be the greater threat because of its design. Active X has direct access to native Microsoft Windows commands. However since Java applets can be attached to e-mail, a browser will automatically activate the applet, enabling Java applet viruses to increase in speed.

Solutions to the security threat of Active X and Java applets are found on both the client side and server side. The most obvious client side solution is to simply disable Java and Active X altogether on user workstations. This solution is less than optimal and acceptable for a few reasons. First, users are accustomed to the multi-dimension control afforder by Active X controls and Java applets. Disabling them will only frustrate the users and disabling them will eliminate some applications of value to users.

There are third party software packages, such as Web Virus Wall, WebProtect, InterScan and Microsoft's Authenticode that will be able to help in the fight against these viruses. These packages are capable of on-off blocking options of controls or applets that may be tampered with. They are also capable of executing the Active X controls and Java applets in an isolated environment, such as a clean room, between the user's computer and the LAN.

At this time, viruses over the Internet by use of Active X and Java applets are isolated. However the concern is growing as security experts and users begin to see a pattern of virus growth that is familiar to the PC viruses.

Internet virus protection policy

The increase in virus incidence despite rising anti-virus software usage can lead to but one conclusion: "It is obvious using existing anti-virus products alone isn't working" (White *et al.*, 1996).

In many cases, the fault lies not in the technology but on the users themselves. If an organization has failed to establish policies for determining how to protect the data from viruses, no product is likely to provide security. Even anti-virus software vendors agree: their products should be used to implement and enforce existing policy, not to compensate for the lack of it (Wood, 1997).

Certainly, products such as anti-virus software are needed to detect and remove computer viruses. Products alone are not enough to solve the problem. A combination of products, people who understand the need for virus protection, and an appropriate procedure for detection could form an effective anti-virus policy (NCSA, 1997; Wack, 1989). Figure 1 shows the key issues that MIS professionals must consider when formulating an anti-virus policy. These issues can be organized into the "three P's" people, products, and procedures (Cohen, 1994; Demey, 1996; Fites, 1989; Slade, 1994; Soloman, 1991).

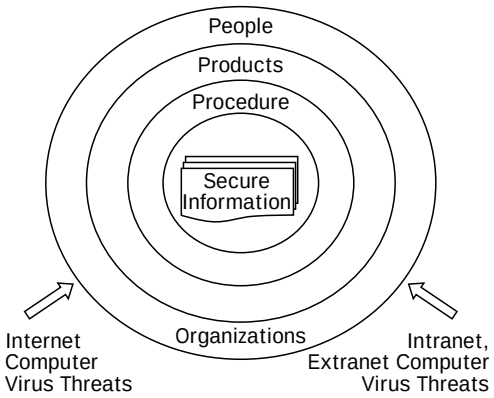
People

The key players in an anti-virus policy are the users and managers inside the company. Two primary steps have to be taken to formulate an anti-virus policy.

Understanding the corporate culture

Corporations have two philosophies on virus protection. There are those corporations that mandate users to inform on all virus detection.

Figure 1
Effective Internet computer virus protection policy



They are required to inform what type of virus was found and by what avenue it was received. The purpose of this is to stop the spread of viruses as soon as possible. Other corporations have a less stringent policy against virus protection. They may only install anti-virus software on users' computers that request it and run virus scans when computer viruses have spread throughout the organization.

User education

Users in the two cases mentioned above need proper education. In the first case, users should be aware of the dangers that exist. They should know what to do if they suspect a security problem. In particular, they should know whom to call and what to do if they have questions or suspicions of having a computer virus. Users should be encouraged to feel that security measures are things that they want to do for their own benefit, rather than things that are required for no rational reason.

Another point making user education important is that, if users are aware of the kinds of visible things that are known to happen in systems that are virus-infected, these users can serve as an important line of defense. Users should know that odd behavior in a computer system may be a symptom of a penetration of a virus.

It is important to educate the end users, the first-level support people, and management involved at all levels, since they must take the necessary actions quickly when a viral infection is detected.

Anti-virus products

The desktop-based solution

Client-based (user-based) anti-virus software, installed on the client's computer, runs when the user boots up the system or when the user explicitly runs the software to perform a virus check on a hard disk or floppy disk. The best desktop products use a combination of detection methods, such as monitoring the system for virus behavior (e.g. formatting the hard disk), comparing files against a database of known virus code, and checking for unexplained changes in file sizes.

However, client-based anti-virus detection methods suffer from a key shortcoming. The client-based periodic approach only detects viruses when the anti-virus software is used by the client. All other files that are downloaded or otherwise transferred into the desktop computer are not checked, each of which may contain a virus.

The server-based solution

A comprehensive virus protection for an entire network depends on scores, if not hundreds, of users employing their desktop protection correctly at all times. Recognizing this obvious flaw, anti-virus vendors developed server-based virus protection five years ago. Server-based virus software resides on the network server. Operating under IPX protocol and NetWare, or in the Windows NT environment, this software protects internal LANs from viruses attached to files that pass through the network server.

Server-based virus protection software is typically more effective than corresponding client-based software. In centralized management of virus protection, scanning is usually more frequent, as is the updating of virus pattern databases that is essential for detecting new viruses.

However, file server anti-virus software suffers from two weaknesses. First, the strong anti-virus capability at the network server rather than the client means that the client is vulnerable to any virus attached to a file that bypasses the network server. Such is the case on the Internet, since downloaded files and e-mail bypass the network server. Second, file server anti-virus software cannot scan e-mail attachments while they are still attached, enabling viruses on these files to spread unchecked.

The "protect all entryways" solution

Both desktop-based and server-based solution alone at best provides limited virus protection for some, but not all network users. Internet-borne viruses are not intercepted by server-based anti-virus software because the connection to the Internet (i.e. the Internet gateway) typically bypasses the network server. This allows viruses to flow into the internal LAN unchecked. Connection to the Internet gateway bypasses the network server because the two use incompatible

protocols and different machines. While network servers typically operate under NetWare using the IPX protocol, 80 percent of all Internet gateways operate under UNIX using the Transmission Control Protocol/Internet Protocol (TCP/IP).

The most effective way to ensure that the internal network remains virus-free is to monitor all entryways for viruses. As shown in Figure 2, using a combination of products that cover every access point – Internet gateways, GroupWare servers, Internet servers, LAN servers, and desktops are the most effective way to protect the network from both the first and the second generation viruses.

For an anti-virus product to be useful, it must reliably intercept viruses without impairing system performance and reliability or user productivity. Configuration and usage flexibility, management capabilities, and customer support are also key considerations when evaluating virus protection.

Putting it together with procedures

While the approach taken to developing an anti-virus policy is likely to vary from company to company, some issues must be addressed in all cases.

Develop anti-virus procedure manual

Procedures are specific operational steps that workers must take to achieve goals – comprehensive virus protection. Procedures are needed for making best use of selected product and service solutions, such as how to install and set up software to take advantage of automatic configuration and deployment, how to customize the level of protection appropriately for different types of user, and, most importantly, how to ensure that regular updates are obtained and deployed to all the workstations.

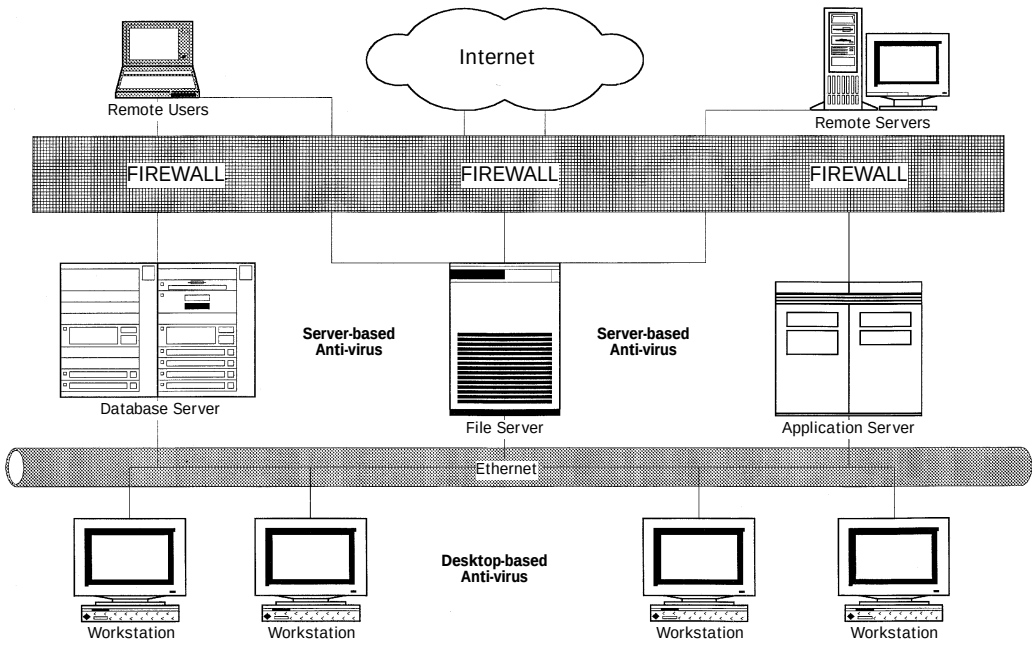
Establish a virus response team

Similar to an emergency response team or other cross-disciplinary group in an organization, a virus response team can be assembled from many different departments. They can be trained and empowered to deal calmly, effectively and professionally with any virus incident. One advantage of such a team is that when an incident does occur, specific people are already selected to immediately tackle cleanup. Of equal importance, providing team members with a specific identity and status sends a message to all employees that virus protection is important and that it involves more than the guys in MIS.

- Upgrade anti-virus product/service. All entryways should be protected with best anti-virus product/service as described before.
- Begin an employee awareness campaign. User education and awareness of the virus threat are a major success factor in the protection policy.
- Periodically review, revise, and reinforce importance of policy.

An annual review is usually sufficient and serves to reinforce an important issue that

Figure 2
The all the entryways solution = Internet firewall + server based antivirus + desktop based antivirus



may not have been discussed for some time. The developed policy must integrate anti-virus products/services, people, and procedures in a manner consistent with the corporate culture, mission and goals. The resulting policy must be clear, concise, and consistent with other corporate policies.

Conclusion

Computer viruses have dramatically increased in complexity over the years. The first viruses were static programs that copied themselves from program to program or diskette to diskette. The viruses that exist today are much more complex. They not only spread the previous ways, but now also spread via e-mail and the Internet. Also a second breed of viruses has been developed – Internet viruses. Their threats to cause destruction are more deadly than viruses that traveled only on LANs. They are the new virus threat that the computer industry needs to direct its fight against and that computer users need to be aware of.

The threat of computer viruses on LANs and PCs is still great. New viruses are being created readily. The PC virus that is most infecting computers today is the Macro virus. Macro viruses are a new wave of viruses that started to appear in 1995 and they are now the most prevalent computer viruses in the world. Macro viruses attach themselves to word processor documents and spread sheets. They spread fast due to the growing use of e-mail attachments.

Viruses can pose a threat to the security of programs and data on computing systems. They can spread without the intent of the people who spread them. Today viruses are spreading new ways. They are spreading over the Internet via e-mail, FTP and now by Active X and Java applets. This means that just browsing the Internet makes the computer vulnerable to viral infection.

The use of anti-virus software to protect against viruses alone is not enough. An effective virus protection policy should combine the "three P's"; people, products, and procedures. In order for policy developers to be successful in their computer virus fight, they should understand the corporate culture, develop an anti-virus procedure manual and begin an employee awareness campaign in the organization. On the IT side they need to establish a virus response team, upgrade anti-virus products on the workstations and servers. Once these suggestions are implemented, they need to be reviewed, revised, and reinforced regularly. Using these suggestions an organization or individual can best protect themselves against computer viruses.

References

Chen, E. (1997), "Active X and Java: the next virus carriers?", *Computer Technology Review*, pp. 38-41.

Cohen, F. (1994), *Short Course in Computer Viruses*, Wiley.

Coursey, D. (1997), "Macro world beyond viruses", *Computer World*, June 2.

Demey, P. (1996), "Protect your electronic data before its too late", *Practical Accountant, December*, pp. 32-35.

Fites, P. (1989), *Computer Virus Crises*, Van Nostranol.

Jarvis, K. (1997), "Demystifying computer viruses", *Management Accounting*, April, pp. 24-31.

Nachenberg, C. (1997), "Computer virus – coevolution", *Communications of the ACM*, January, pp. 46-51.

New York Times (1993), "The virus: threat or menace?", *New York Times*, 15 June.

NSCA (1997), "NCSA® 1997 computer virus prevalence survey", NCSA, available at http://www.antivirus.com/forms/ncsarep.html

Slade, R. (1994), *Guide to Computer Viruses*, Springer-Vaelag.

Soloman A. (1991), *PC Viruses: Detection, Analyses and Cure*, Springer-Valag.

Wack J. (1989), *Computer Viruses and Related Threats: A Management Guide*, Department of Commerce.

Whalley, I. (1996), "Virus defense for the future", *Security Management*, November, pp. 60-4.

White S.R., Kuo, C.J. and Chess, D.M. (1996), *Coping with Computer Viruses and Related Problems*, IBM Los Angeles Scientific Center and IBM Thomas J. Watson Research Center.

Wood C.C. (1997), "Policies from the ground up", *Infosecurity News*, March/April, pp. 24-8.